DOI 10.37882/2223-2974.2024.05.35

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Тощук Сергей Николаевич
Аспирант, Ростовский государственный экономический университет
toshchuk@yandex.ru

Аннотация. В данной статье рассматривается важная тема нормативного регулирования, которая направлена на обеспечение безопасности систем промышленного интернета вещей (IIoT). Обеспечение безопасности IIoT является критически важным, так как угрозы безопасности систем IIoT могут привести к серьезным последствиям для организаций и общества в целом. Статья содержит анализ текущего состояния нормативного регулирования в области безопасности IIoT, включая международные и национальные стандарты, рекомендации и обязательные требования. Дан анализ российскому нормативному регулированию безопасности систем IIoT. Рассмотрены различные технические меры обеспечения безопасности систем IIoT. Разработаны некоторые рекомендации по обеспечению безопасности систем IIoT.

Ключевые слова: промышленный интернет вещей, информационная безопасность, нормативное регулирование, технические меры, анализ подходов, международные нормативные акты.

REGULATORY REGULATION OF ENSURING THE SECURITY OF INDUSTRIAL INTERNET OF THINGS SYSTEMS

S. Toschuk

Summary. This article discusses an important topic of regulatory regulation, which is aimed at ensuring the security of industrial Internet of Things (IIoT) systems. Ensuring the security of IIoT is critically important, as threats to the security of IIoT systems can lead to serious consequences for organizations and society as a whole. The article contains an analysis of the current state of regulatory regulation in the field of IIoT security, including international and national standards, recommendations and mandatory requirements. The analysis of the Russian regulatory regulation of the safety of IIoT systems is given. Various technical measures to ensure the safety of IIoT systems are considered. Some recommendations have been developed to ensure the security of IIoT systems.

Keywords: Industrial Internet of Things, information security, regulatory regulation, technical measures, approaches analysis, international regulatory acts.

По мере развития сети Интернет, человеческая цивилизация вышла на такой уровень управления отдельными устройствами в отраслях экономики, как IIoT-системы.

В 1999 году К. Эштон ввёл определение «Интернет вещей» (ИВ). С развитием сети Интернет этот исследователь полагал, что окружающие человека предметы будут со временем объединены в сеть Интернет с помощью особых датчиков и линий связи, что позволит такой системе функционировать вне непосредственного человеческого участия [1].

Однако, по прошествии четверти века так не сформировалось в научном сообществе общего для всех подхода к такому понятию.

В некоторых международных документах упор делается на глобальный характер инфраструктурной системы, в которой элементы связаны между собой с применением различных технологических решений. В этом заключается основная проблема, как объединить и управлять разнородными предметами в информационном пространстве, имея разнообразные средства коммуникации [2].

В программном документе Российской Федерации [3], к ИВ отнесены факторы информатизации отдельных предметов и их объединение в единую сеть для получения необходимого социально-экономического эффекта для отдельного потребителя, групп потребителей и всего общества.

С учётом сказанного, мы можем определить некоторые признаки, присущие Интернету вещей. Таких вещей (предметов, объектов) имеется значительное количество. Происходит накопление разнообразных данных в вещах (предметах, объектах), касающихся своего состояния и внешней среды.

Производится взаимная передача накопленной информации между соединёнными линиями связи вещами, предметами и объектами. Описанные функции осуществляются вне непосредственного человеческого участия. Реализуемые функции имеют юридические последствия для всего российского общества.

Использование в российском обществе IIoT-систем предусматривает, что описанные категории и отношения происходят в какой-то отрасли промышленности или производства, а не в человеческом быту.

На настоящий момент, IIoT-системы представляют собой коммуникационную сеть устройств, оборудования и систем, которые собирают, обрабатывают и обмениваются данными в промышленных условиях для оптимизации производственных процессов и улучшения качества продукции. В IIoT-системах используются сенсоры, устройства автоматизации и другие технологии для связи физических объектов и процессов в единую систему управления и мониторинга [4].

Как и любые системы, так и наши IIoT-системы имеют большую нужду в безопасности. В связи с чем это обусловлено? Потому, что в результате кибератак по линиям связи на систему IIoT допуск к ней может быть взломан, в результате чего в систему внедряется вредоносное программное обеспечение или производится кража данных. Такие данные могут относиться к коммерческой, технической или персональной тайне, не подлежащей разглашению лицам, не допущенным к ней.

Дальше, по цепочке, нарушения в IIoT-системах повлияют на снижение производительности оборудования, вызовут материальные или временные потери, или простои техники и персонала, потери конкурентного положения ряда компаний на рынке IIoT-систем.

Если IIoT-системы входят в состав критической инфраструктуры, к примеру, в энергетику или транспорт, то ущерб может быть значителен, выходящий за пределы отдельной отрасли или государства [5, 6].

И поскольку также в IIoT-системы активно внедряются программные комплексы на основе искусственного интеллекта (ИИ), то на уровне международного права были приняты стандарты и регламенты в сфере ИИ и IIoT.

Рассмотрим правовые аспекты информационного обмена между предметами в IIoT-системах. Прежде всего, приходится передавать значительные объемы информации, которые можно охарактеризовать как «Большие данные», которые в свою очередь отличаются разнородностью, скоростью передачи и обработки, и объёмами.

Такие данные объединяются в правительственные, общественные, частные, личные базы данных в зависимости от статуса собственника и (или) пользователей IIoT-систем. Указанная информация подвергается особой обработке с целью определения состояния отдельных объектов, системы в целом и окружающей среды, что влечет за собой правовые последствия.

Отмечаем, что, особенно в последние годы, IIoT-системы бурно развиваются. Прогнозируем, также, что за 12 лет с 2015–2027 гг. количество таких устройств вырастет в три раза, к 41 млрд штук.

Россия в условиях международного ограничения в сфере передовых критических технологий создает новые IIoT системы. Однако, внутренний промышленный рынок потребителей новых товаров и услуг не является широко развитым в силу дороговизны и не очень широкой доступности новых технологий.

Большая часть производственных ресурсов направлена на решение текущих задач, в том числе, в сфере военной индустрии. Правовые отношения с участниками рынка сферы IIoT не всегда урегулированы в полном объеме. Иногда это выходит за рамки государственной границы в зарубежные юрисдикции.

Интернет — это глобальная инфраструктурная система, потому и вещи, предметы, вовлеченные в нее, так же перестают быть личными или частными, а попадают в глобальное использование, в том числе, и к недружественным лицам и юрисдикциям. Недружественные к РФ страны своей санкционной политикой создают международную правовую среду, препятствующую развитию в нашей стране систем IIoT.

Несмотря на это, мы наблюдаем, насколько активно развивается Интернет-поколение 5G, ИИ и граничные вычисления в стране и в мире [5]. Системы с IIoT являются лидерами по сравнению с другими направлениями по развитию и уровню финансирования.

В нашей стране системы с IIoT внедряются в медицину, в энергетику, в животноводстве и растениеводстве, в транспорт и грузооборот, в жилую и городскую инфраструктуру, что приблизится в финансовом выражении к трём трлн. руб. Успешность такого внедрения обеспечивается системой государственной поддержки.

Прогрессивным шагом является развитие программ по совершенствованию сетей связи системы с IIoT по всей стране [7]. В данном процессе шлифуются и стандартизируются технологии по мере внедрения пробных проектов в жилую инфраструктуру, в здравоохранение, в животноводство и растениеводство, и т.д.

Поскольку все больше и больше слоев и категорий населения вовлекаются в использование системы с IIoT, то возникает объективная необходимость совершенствование правовых отношений, связанных с этими вопросами. Прежде всего это касается регулирование отношений, связанных с отношениями собственности.

Как генерируется, хранится, передается и смешивается информация, которая принадлежит субъекту? В последние годы, потребители привыкли свою наиболее ценную информацию хранить в электронном виде на внешних зарубежных серверах, что не является полностью безопасным решением при нестабильности в международных отношениях.

Как этой информацией может пользоваться другой субъект или субъекты?

Любой субъект, зная логин и пароль допуска к информации, может воспользоваться этим, и это не всегда идет на пользу собственнику информации.

Как защитить такую информацию?

Методы и способы информационной защиты способны это совершить.

Как определить ущерб в связи утечкой информации и степень ответственности злоумышленника, организовавший такую утечку?

Недополученная прибыль, падение рейтинга компании на рынке, создание конкурентами аналогичной продукции. Степень ответственности определяет суд. Важно, чтобы международный и национальный суд следил за выполнением своих ответственных решений.

Современное законодательство в информационном мире не всегда адекватно квалифицирует все возникающие коллизии вокруг IIoT-систем.

Возможно ли в этой сфере следует радикально переработать действующее законодательство?

На наш взгляд, это возможно. Нам представляется важным выделить несколько важных правовых аспектов. Информация, циркулирующая в IIoT-системах, имеет IIoT конфиденциальный, личный или персональный характер. Это не только телеметрическая информация, но и данные, которыми не все готовы поделиться.

IIoT-системы иногда передают не только информацию, полученную от собственных датчиков, но и обрабатывают данные с вышестоящего уровня управления, и, тем самым, нуждаются в правовой и технической защищённости такой информации.

Поскольку в этот процесс вовлекается ИИ, то ответственные решения за людей принимают программные комплексы, что вызывает правовые, социальные, экономические последствия таких процессов и решений. И потому, в складывающихся условиях возможны появления новых вредоносных деяний, которые нуждаются в квалифицированной правовой оценке.

Известно, что в международной юрисдикции действуют некоторые нормативные документы, так или иначе регулирующие циркуляцию данных в IIoT.

Перечислим такие документы: GDPR, NIST Cybersecurity Framework, IEC 62443, ISA/IEC 62443 и другие документы, затрагивающие сферу IIoT по всем вопросам, которые волнуют производителей и потребителей в указанной сфере.

Документ IISF, разработанный IIC, наиболее всего отвечает потребностям безопасности IIoT-систем [8].

В 2019 г. разработаны «Рекомендации по искусственному интеллекту», что позволило определить подходу к разработке и использованию искусственного интеллекта для различных сфер его применения [9]. Данный документ является межгосударственным стандартом в сфере ИИ.

В 2020 г. составлена «Белая книга по искусственному интеллекту», которая отражает принципы ЕС по использованию ИИ в новых технологиях [10].

В тот же год была предложена новая европейская стратегия, которая затрагивает проблемы использования и защиты информации, о правах потребителей и о борьбе с монополиями, что заложила основы современной экономики данных в ЕС [11].

В последующем, был принят новый регламент, в котором определены процедуры использования данных, которые циркулируют в ЕС, и новое европейское законодательство по исследуемой проблематике [12,13].

Германия, как экономический лидер Европы, в очередной 4-той версии стратегической программы, определила вопросы информационной безопасности для IIoT-систем. Кроме того, Федеральное министерство экономики и энергетики (BMWi) ФРГ совершенствует технические рекомендации и стандарты для безопасности IIoT-систем.

Рассмотрим законодательные инициативы, касающиеся сферы IIoT, за пределами ЕС. Министерство промышленности и информационных технологий (MIIT) КНР выпустило несколько руководств и рекомендаций по безопасности IIoT.

В Японии существуют рекомендации, направленные на разработку стандартов и руководств по безопасности IIoT-систем. Так, японская ассоциация промышленного интернета (JIIA) разрабатывает рекомендации по безопасности IIoT-систем.

Такие немногочисленные примеры свидетельствуют о том, что мировое сообщество находится только в начале правового разрешения проблем безопасности в IIoT-системах. Насколько каждая страна развита экономически и в правовом отношении, настолько это влияет на правую защищённость национальных IIoT-систем, исходя из технологических возможностей таких стран [14].

Поэтому в Российской Федерации (РФ) принята государственная программа о цифровой экономике. Данный документ направлен на развитие инновационных и информационных, в том числе, ИИ и IIoT-технологий [15].

Перспективы развития ИИ и IIoT представлены в материалах национальной стратегии и в указах [19, 20], что является правовыми вехами при переходе российской экономики в более инновационное состояние.

В 2019 году законодательство в РФ было пополнено новым государственным проектом, улучшающим цифровую сферу [18]. Следующий документ стратегического планирования затронул сферу развития ИИ до 2030 года [16].

В интересах развития в РФ инновационных технологий в информационной сфере в 2020 году принята новая Концепция с горизонтом планирования четыре года с учётом юридических аспектов указанной деятельности [17].

Среди правовых документов РФ по защите информации в системах IoT отмечаем Федеральный закон «О защите информации» (ФЗ-187). ФЗ 187 «О защите информации» и приказы ФСТЭК 31, 235, 239 задают общие требования и рекомендации, и не являются специфическими нормативно-правовыми актами, ориентированными исключительно на IIoT. Регламенты безопасности предлагаемых на рынке РФ товаров и услуг определены в Федеральном законе, защищающем сторону потребителей [21].

Однако, для полноценного нормативного регулирования безопасности IIoT может потребоваться дальнейшая разработка специальных нормативно-правовых актов, которые учитывают специфику и особенности промышленного Интернета вещей в Российской Федерации.

ЛИТЕРАТУРА

1. Ashton, K. That «Internet of Things\'Thing» // RFID Journal. 22 June 2009.
2. Рекомендация Международного союза электросвязи МСЭ-Т Y.2069 «Серия Y: Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений. Сети последующих поколений — структура и функциональные модели архитектуры. Термины и определения для интернета вещей». Издание 1 от 29.07.2012.// Сайт «International Telecommunication Union». — Режим доступа: https://www.itu.int/rec/T-REC-Y.2060-201206-I (дата обращения: 01.12.2023).
3. Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года (разработан Минэкономразвития России) // Официальный сайт Министерства экономического развития РФ. — Режим доступа: http://www.economy.gov.ru по состоянию на 30.04.2013 (дата обращения: 01.12.2023).
4. Haller, S., Karnouskos, S., & Schroth, C. (2015). The industrial internet of things: Challenges, opportunities, and directions. In Internet of things (pp. 1–14). Springer.
5. Kaur, R., & Kaur, A. (2019). Security issues and challenges in industrial internet of things (IIoT): A comprehensive review. Journal of Ambient Intelligence and Humanized Computing, 10(3), 1127–1151.
6. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.
7. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497–1516.
8. Ziegeldorf, J.H., Morchon, O.G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728–2742.
9. Recommendation of the Council on Artificial Intelligence // Режим доступа: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (дата обращения: 01.12.2023).
10. White Paper on Artificial Intelligence: a European approach to excellence and trust // Режим доступа: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (дата обращения: 01.12.2023).
11. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region a European strategy for data// Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020 DC0066 (дата обращения: 01.12.2023).
12. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868/(дата обращения: 01.12.2023).
13. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN/(дата обращения: 01.12.2023).
14. Perera, C., Liu, C.H., Jayawardena, S., & Chen, M. (2017). A survey on Internet of Things from industrial market perspective. IEEE Access, 5, 3610–3632.
15. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7.
16. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года».

17. Распоряжение Правительства РФ от 19 августа 2020 г. № 2129-р об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.
18. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7.
19. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года».
20. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».
21. Антипова, К.Г. Вопросы правовой квалификации больших данных как цифровых активов // Юридические исследования. — 2022. — № 11. — С. 45–61. DOI: 10.25136/2409-7136.2022.11.38928 EDN: VYZDVX Режим доступа: https://nbpublish.com/library_read_article.php?id=38928 (дата обращения: 01.12.2023).

Журнал «Современная наука: актуальные проблемы теории и практики»